REMARKS

This is in response to the Office Action mailed on March 25, 2004. Claims 37-44 were pending in the application, and the Examiner rejected all claims. With this amendment, claims 37, 39, 40 and 42 are amended and the remaining claims are unchanged in the application.

On page 2 of the Office Action, the Examiner objected to claim 42 based on two informalities, and suggested amendments to the claims. In accordance with the Examiner's suggestions, claim 42 has been amended and Applicant thus believes claim 42 is in proper form.

At the bottom of page 2 of the Office Action and the top of page 3, the Examiner rejected claims 37-44 under 35 U.S.C. §112, second paragraph, as being indefinite. The Examiner indicated that it was unclear whether the phrase "message specific data derived from the information to be transmitted" referred to data that was specific to the transmission message or merely data that was derived from the information to be transmitted. In accordance with the Examiner's suggestion, Applicant has amended the recitation "message specific data" to "transmission message specific data." Applicant thus believes that the claims are now clear.

On pages 3-8 of the Office Action, the Examiner rejected claims 37-44 under 35 U.S.C. §103(a). Of those claims, claim 37 in an independent claim, and the Examiner rejected it based on a combination of four different references (the ETS reference, the Brown et al. patent, the Moore patent, and the Schneier reference). Applicant respectfully traverses the Examiner's rejection.

None of the four references combined by the Examiner, either alone or in combination, teach or suggest the present invention as set out in independent claim 37. Further, Applicant submits that it would not be obvious to combine the references as suggested by the Examiner.

The references simply do not teach or suggest the present invention. For instance, none of the references either alone or in combination teach using two keys during the encryption process wherein both of the keys are derived based on a base key, message independent data (such as encryption data 246 or signing data 264) and message specific data. In fact, the only reference which even discusses using two keys to encrypt a message is the Moore Patent.

Not only does Moore encrypt a message in an entirely different way than that set out in independent claim 37, but Moore makes no mention, whatever, as to how the two encryption keys are generated. Not only is Moore silent as to how the keys are generated, Moore specifically fails to teach that the keys are generated by first and second encryption key components that hash message specific data, message-independent data and a base key. The other references do not remedy this deficiency.

Brown et al. specifically teaches only the use of a single encryption key during encryption of messages. Brown et al. neither teaches nor suggests how the encryption key is generated. Brown simply states that a packetized message encryption key is generated. See column 7, lines 64-67. Brown et al. further states that the packetized message encryption key is used to encrypt the message packet, which is eventually sent. See column 8, lines 10-16.

Brown also discusses a separate authentication process during which a single session key is generated based on first and second shared secret data, random challenge data, and instant-specific information. While it is unclear from the reference, it would appear that none of this information is message specific data or a base key. Brown et al. does not mention a base key for use in generating a session key, and the "instant-specific" information would appear to be the same for any message created at a given instant, regardless of the message content. Therefore, Brown et al. does not teach generating a key from a base key and message specific data.

The ETS reference does not teach or suggest generating even one key based on message specific data or from a base key. Instead, ETS simply teaches a method of transferring an agreed upon key (K_c) from a network to a mobile station. To do this, a network sends a "RAND" authentication value (which is not message specific data, but is, in fact, a non-predictable number) to the mobile station. K_c is derived from RAND and the subscriber authentication key K_i. See sections 3.2 and 3.3. Thus, the ETS references fail to teach or suggest generating even one encryption key (much less two) from message specific data and a base key.

The Schneier reference simply discusses a key-dependent hash function. It simply does not teach or suggest generating even one encryption key (much less two) in a message transmission system based on message specific data and a base key.

Applicant thus submits that none of the references, either alone or in combination, teach or suggest either of the first and second encryption key components set out in independent claim 37, much less both of those components in combination.

Further, none of the references either alone or in combination teach generating an encrypted message in the same way, using the same components, as that set out in claim 37. Specifically, claim 37 states that the encryptor is configured to hash information to be transmitted with the first encryption key in order to obtain a signature and to encrypt the information and the signature with the second encryption key to obtain an encrypted message. Claim 37 further includes a joiner configured to join the encrypted message with the transmission message specific data in unencrypted form. One illustrative embodiment of this is shown in FIG. 11A. None of the references teach or suggest this system.

As set out above, the ETS system simply discloses a system by which a non-predictable number (RAND) is sent to a mobile station from a network. Brown teaches sending encrypted information as shown in Brown's FIG. 5 by generating a packetized message encryption key, encrypting the message packet and sending it. See column 7, lines 64-67, and column 8, lines 10-16. Also, as mentioned above, the Schneier reference simply teaches a key-dependent hashing function.

In addition, the Moore patent fails to teach or suggest the system set out in claim 37 as well. The Moore patent discloses a system which attempts to ensure that software is authentic, when received from a re-use library. Moore encrypts a plain text version of software and then hashes it. Moore then encrypts the hash result and the original encryption key with a second encryption key. In the re-use library, Moore stores the encrypted software, the encrypted hash result, and the encrypted first key. Thus, Moore is related to a fundamentally different type of system than the transmission system for transmitting information to a mobile device set out in claim 37. Similarly, there is no teaching or suggestion in Moore that the message data is first hashed to obtain a signature and that the signature and the original message data are then encrypted using an encryption key. This is simply not discussed or suggested, in anyway, by Moore. Nor does Moore teach or suggest the joiner from claim 37 which joins the encrypted message and the unencrypted message specific data.

Since the features discussed above are neither taught nor suggested by any of the references cited by the Examiner, either alone or in the 4-way combination provided by the Examiner, Applicant submits that independent claim 37 is allowable over the references.

Applicant further submits that it would not be obvious to combine the references as cited by the Examiner. The references are directed to fundamentally different systems. Schneier simply teaches a hashing function, Moore teaches a re-use library software authentication system, the ETS reference and the Brown et al. patent are directed to communication systems. There is no suggestion in any of the references that they should be combined as suggested by the Examiner.

Instead, we would respectfully submit that the Examiner is using independent claim 37 as a blueprint to pick and choose isolated discrete teachings from the bodies of the four diverse references in order to assemble them in the particular way taught by independent claim 37, where there is otherwise no objective reason to combine those specific features in the specific way suggested by the Examiner. Applicant thus submits that the specific combination of the isolated features of the four references cited by the Examiner is neither taught nor suggested by any of the references cited by the Examiner, nor is the combination obvious, without using claim 37 as a starting point. Applicant thus submits that independent claim 37 is allowable over the references cited by the Examiner.

Dependent claims 38-44 depend either directly or ultimately from independent claim 37. Therefore, Applicant submits that those claims are allowable as well.

In conclusion, Applicant submits that claims 37-44 are in proper form and are allowable over the references cited by the Examiner. Reconsideration and allowance of claims 37-44 are respectfully requested.

The Director is authorized to charge any fee deficiency required by this paper or credit any overpayment to Deposit Account No. 23-1123.

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By: Joseph R. Kelly

Joseph R. Kelly, Reg. No. 34,847
Suite 1600 - International Centre
900 Second Avenue South
Minneapolis, Minnesota 55402-3319
Phone: (612) 334-3222 Fax: (612) 334-3312

JRK:slg